József Bokor

An introduction to the examination of security issues in cyber-physical systems

József Bokor, full member of the Hungarian Academy of Sciences, Vice President of the Hungarian Academy of Sciences, Scientific Director of the Institute for Computer Science and Control of the Hungarian Academy of Sciences

Introductory thoughts concerning the subject of cybersecurity and cyber-physical systems

The virtual space – the so-called "cyberspace" –, made up of interconnected computer networks, has undergone an unprecedented expansion during the past decade. To an ever increasing extent, state and government bodies, companies and individuals require the ability to integrate the benefits of their online presence into their daily activities. The *World Wide Web (WWW)* has been the predominant technology for the past several decades to share electronic content around the world and retrieve it according to specific criteria. The enabler of leveraging the technology and making it accessible globally to everyone was made possible by the improvement of quality and reliability of the underlying technologies (e.g. network building and server technologies, virtual machines).

As the spatial expansion of cyberspace continues and the density of its supporting resource systems increases in the technologically advanced regions of the world, maintaining the reliability of services and the security of contents turned out to be the greatest challenge ever for the traditionally open and innovative digital technology, offering open access for everyone. At the same time, the advanced engineering systems of the future that emerged in the recent years are a product of a symbiotic approach to process control and informatics, creating a qualitatively new situation in the area of technologies previously described only as safety critical. Traditionally, safety critical systems are described as *standalone* engineering systems and applications the operation of which come with inherent risks of life threatening accidents and/or serious damages to the economy, the environment or even the society if they malfunction. Such systems include vehicle and aircraft control, applications in the chemical industry and in nuclear power plants, but also banking applications.

Cyber-physical systems are safety critical systems operating in the cyberspace: their physical implementation involves (embedded) computers, with a complicated network of connections between them, that collect data over various networks, monitor and control complex physical processes, manage sensors and actuators. The prevalent applications of

cyber-physical systems have a significant impact on our daily lives thanks to the exceptional degree of their adoption by the society: they can have a profound influence on our quality of life and on the efficiency of the contribution of industry, healthcare, education, and any other systems that are part of the private sector, and/or of an economic player to the national economy; they determine the state of the environment and the general conditions of community work. However, if they malfunction or if they deliver corrupted or maliciously altered content, these system may also be capable of causing accidents claiming human lives, service disruptions in entire regions, damages to properties, and environmental disasters, and as such they should be regarded as systems and technologies that have national security related implications, belonging to the critical infrastructure, and should be prioritized both in the design stage and in operation. For this reason, protecting the critical infrastructure has become a primary objective of modern societies. Technological progress comes with a number of benefits and opportunities, but it also carries new security risks and social challenges. Implementation and sustainable operation of cyber-physical systems introduce new challenges in terms of protecting the security of the cyberspace.

The *number of risk sources* or, in other words, the *threat* increases in proportion to, or – according to certain opinions – at a rate significantly exceeding the growth of the size of networks, which can be explained by the fact that the root causes of emergencies are mostly coded into the technological systems as structural sources of faults and failures. Operation in an incorrectly selected architecture carries structural risks. The *risk degree* has a distribution pattern that shows geographically varying densities, and is related to how advanced the local technology is. The fluctuations in the density distribution of services are characterized by the inherent proclivity of *large-scale* networks to form hubs as a result of their *(scale-free)* network organization and growth characteristics. Over the conventionally fault-tolerant, highly distributed connection systems of the Internet a highly vulnerable service delivery system built on centralized distribution/service hubs is formed, which increases the interdependence of system elements, and requires a system-level approach to the handling of vulnerabilities.

Reducing the openness of the system cannot be used to increase the security of cyber-physical systems as the operation of these systems rely on uninterrupted connectivity, which is characterized by a pool of redundant and highly distributed resources and cooperative task execution. One of the most important questions is how risks can be reduced by implementing security measures to block attempts at disabling or impairing technologies without restricting openness and accessibility that are regarded as essential in the context of those technologies and the society.

Preventive and countermeasures can be divided into two major groups. There are so-called *design-stage* considerations and there are *operational-stage* methods that can be applied to the operation of the rolled-out systems. For example, it is a design-stage consideration that the least vulnerable and self-repairing architectures should be created. When the architecture of cyber-physical systems with significant operational risks is designed, the security analysis, that is part of the design process, will involve maximizing the permissible statistical frequency (risk) of malfunction by a probability value proportional to the amount of damage caused, requiring that the probability of an unwanted event should never exceed this threshold.

In order to meet security requirements, the most critical cases may necessitate the use of fault tolerant solutions. Fault tolerance is the property of a system that allows it to restore its original functionality by recognizing anomalous changes in its operation (resulting from malicious interventions, tampering with data, component failures or any other external effects that have an impact of any kind on the integrity of the system). Fault tolerance, as a design property of the system, is an autonomous operational feature based on the detection of faults and failures and any other unwanted changes, aiming at restoring normal operation immediately.

Up until recently security issues of cyber-physical systems providing critical functionality were addressed typically in the area of network infrastructure protection and fault-tolerant control design. *Accuracy, integrity*, and *reliability* of data collected and processed by the system and their impact on security were given little though in the evaluation of risk factors. The status of sensors and actuators and their interaction with the environment containing the system were not a key part of investigations. This practice led to security solutions that assumed a closed cyberspace where the origin of faults and attacks was likely to be found inside the cyberspace (or, as a matter of fact, in the connection between computers). This approach is well characterized by the fact that, for example, while cryptographically encoded and authenticated *(digitally signed)* data traffic between communication end-points offers a solution for securing communication between two parties in a way that is literally unbreakable within a reasonable period of time and provides efficient defence against unauthorized injection of new data content between the two end-points, it is powerless against the malicious modification of transmitter-side sensor data (or the immediate physical environment of the sensor itself).

Thus, cyberspace should be regarded as an integrated whole containing sensors, actuators, information and network systems; a space with problems that cannot be resolved from the inside without taking into account processes in the environment encapsulating it. This way of looking at the problem may facilitate the handling of security risks in systems by correctly determining their vulnerability directions and treating their security risks as part of their environments, following a *systems theoretic* approach.

As a result, plausibility problems *(trusting)* that were brought up earlier in regard to the malicious tampering of measurement data and the reliability of sensors, should also be addressed as part of a new approach. For example, how can someone be sure that data entering the system provide an authentic representation of reality? Conventional error detection mechanisms of sensor systems which are based on testing the statistical independence of measurement data, are suitable for pinpointing physically damaged sensors or sensors that failed for any other reasons, and isolating data supplied by them. However, these methods cannot be applied to stop sophisticated attacks against the sensor space itself. In order to achieve this goal, new systems that are capable of verifying the plausibility of data must be used.

Through the application of the advanced methods of data science and machine learning, patterns, fingerprints, and regularities indicating normal operation can be extracted from the data entering the system, and then they can be used to detect anomalies. These topics are discussed in the first part of the study in which the author, András Benczúr, applies one of the most advanced methods of data science, the so-called *big data,* to the problem of input plausibility. In doing so, he elaborates the possibilities of the so-called data-driven

methodologies (methods using computer-based analysis and modelling of data) in the detection of security risks. Big Data based, typically real-time analytic processes, however, can only be implemented efficiently on an elastic IT infrastructure that offers versatility of access and support for custom configurations. The distributed method of data access, data sharing between the active elements of the system performing the analysis, and cooperative processing lay down the foundations of employing new plausibility checking methods based on the diversity of sources, and as a result, creating robust fault-tolerant systems. Design methods of this infrastructure *(IT cloud)* and the issues of implementing the Bid Data concept are addressed by Róbert Lovas in the second part of this chapter.

In cyber-physical systems, resolving input plausibility issues is a topic subject to real-time constraints. In such cases, control tasks should be taken over by efficiently distributed management and filtering strategies that are suitable for the architecture of the system. Environment perception methods for autonomous vehicles and vehicles systems, such as camera vision based methods, LIDAR (laser) based environment perception technologies, and complex shape, movement and human detection applications ensuring the accuracy of positioning and monitoring community spaces exposed to risks, represent serious scientific challenges in terms of compliance with security requirements. Such problems, including the capabilities and the applications of leading environment perception methods and a presentation of the typical signals and signal processing devices are discussed by Szirányi and Havasi in the third part of this chapter.

The automated transport systems of the future will form an emerging new class of critical infrastructures that, due to the overarching character of the transport sector within the national economy, play a fundamental role in ensuring the security of systems and processes affecting the entire society. Special applications of automated transport systems can be implemented in the domain of driverless ground and aerial vehicles. An overview of the research and development directions of controlling small flying objects that are usually not subject to a permit to fly (drones or UAVs) and the security aspects of integrating these vehicles into the air traffic control system is provided in the closing part of our chapter, by the authors József Bokor and Bálint Vanek.